VAASAN AMMATTIKORKEAKOULU
VASA YRKESHÖGSKOLA
UNIVERSITY OF APPLIED SCIENCES

Joonas Herronen

# Tietoturvakartoitus pk-yritykselle

Toimialayksikkö Liiketalous ja matkailu

2013

VAASAN AMMATTIKORKEAKOULU
Liiketalous ja matkailu

# TIIVISTELMÄ

| | |
|---|---|
| Tekijä | Joonas Herronen |
| Opinnäytetyön nimi | Tietoturvakartoitus pk-yritykselle |
| Vuosi | 2013 |
| Kieli | suomi |
| Sivumäärä | 37 |
| Ohjaaja | Antti Mäkitalo |

Lopputyö käsittelee tietoturvaa ja sen merkitystä pienessä Vaasalaisessa pk-yrityksessä. Toteutin työni syksyn 2012 ja kevään 2013 aikana.

Työssä on tarkoitus selventää tietoturvan standardeja, AEO-sertifikaatin tietoturvaan liittyviä vaatimuksia, sekä suorittaa yritykselle tietoturvaan liittyvä kysely ja selvittää tämänhetkiset käytössä olevat atk-laitteet. Lisäksi laadin pienen yleisen tietoturvaohjeen yritykselle.

Työssäni selvisi, että päivittäinen tietoturva ei ole aina yritykselle itsestään selvyys, vaan se tarvitsee ohjeistusta ja hyvin mietittyjä toimintamalleja. Hyvällä selvitystyöllä ja koko yrityksen tekemisellä AEO-vaatimukset saadaan kuitenkin selville ja täytettyä. Pienen yrityksen kohdalla ei ole välttämätöntä hakea todistusta, jos ei ole esimerkiksi omaa vientiä ulkomaille, että voitaisiin hyödyntää tullihelpotuksia.

Avainsanat tietoturva, AEO, standardit

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
VAASAN AMMATTIKORKEAKOULU
Liiketalous ja matkailu

# ABSTRACT

| | |
|---|---|
| Author | Joonas Herronen |
| Title | An Information Security Research for a Medium-sized Business |
| Year | 2013 |
| Language | Finnish |
| Pages | 37 |
| Name of Supervisor | Antti Mäkitalo |

This thesis includes information about security and its role in A small company located in Vaasa. The work was accomplished between autumn 2012 and spring 2013.

In the work, the focus was on information security standards, AEO-certificate demands and also a small survey was made about information security for the case company.

The main result of the study was that a medium-sized business can not take information security for granted but they must give resources to security. However, with good research work AEO demands can be completed. One of the main results of the study was also that a small company does not need an AEO-certificate if they do not need customs services.

Keywords Information security, AEO, standard

# SISÄLLYS

**SANASTO**

AEO = Authorised Economic Operator - maailmanlaajuinen hanke, jonka tavoitteena on edistää kansainvälisten toimitusketjujen turvallisuutta.

Auditointi = Objektiivinen ja määrämuotoinen arviointi, jolla selvitetään, täyttääkö joku tietyt vaatimukset.

Phishing = Verkossa tapahtuvaa rikollista toimintaa, jolla pyritään saamaan haltuun esimerkiksi luottamuksellisia tilitietoja.

Proxy = Välityspalvelin, jota käytetään ensisijaisesti WWW-sivujen varastoimiseen.

Roskaposti = On sähköpostitse tapahtuvaa luvatonta massapostitusta.

Sertifikaatti = On todistus, että jokin asia on käytössä

Tietoturva = On palvelujen, tietojen, järjestelmien ja tietoliikenteen suojaamista.

Fyysinen tietoturva = Tarkoittaa toimitilojen ja siellä olevien laitteiden suojaamista.

Organisaatio = Pk-yritys, joka tilasi työn.

Kultainen kädenpuristus = Rahallinen lahja irtisanotulle, ettei tietoa vuotaisi tai jos irtisanominen on ollut muuten nopea tai sopimuksen vastainen.

# JOHDANTO

Tietoturva tuntuu olevan monelle pienelle pk-yritykselle vaikeasti hallittavaa alue, koska yrityksillä ei ole resursseja pitää vakituista atk-henkilöstöä. Yleensä alihankkijoina toimivilla pk-yrityksillä isot asiakasyritykset määrittelevät tiettyjä vaatimuksia alihankkijoilleen ja he luovat yhdessä lainsäädännön kanssa yritykselle tietoturvan minimitason. Työssäni tarkoitukseni on selvittää pk-yrityksen tietoturvan tasoa sellaisessa skenaariossa, jossa yrityksellä ei ole kokopäiväistä atk-henkilöä töissä. Yrityksessä toivottiin myös lyhyitä ja selkeitä tietoturvaohjeita päivittäiseen toimintaan. Näiden avulla voidaan varmistaa että sekä oman organisaation, että asiakkaiden salassa pidettävät asiakirjat pysyvät suojattuina ja tietoturva vaaditulla tasolla.

Toimeksiannon tehneellä pk-yrityksellä tietoturvaa koskettaa ison asiakkaan saama AEO-sertifikaatti, jonka mukainen toiminta vaatii yritykseltä tietoturvaan panostusta ja asettaa vaateita koskien yrityksen toimintaa. Pk-yrityksen pitäisi täyttää AEO-sertifikaatin minimitaso ja lähteä kehittämään toimintaansa siitä eteenpäin.

Yritykselle ei ole aikaisemmin tehty tietoturvakartoitusta, vaikka se on toiminut jo 20 vuotta. Tarkoituksena on selvittää toimeksiantajalle yrityksen nykyinen tietoturvataso. Selvitettyäni yrityksen tietoturvatason peilaan sitä AEO- sertifikaatin asettamiin minimivaatimuksiin. Näin voidaan tuoda tietoon tietoturvapoikkeamat ja mahdolliset parannusvaihtoehdot. Toinen tarkoitus on kyselyn pohjalta miettiä, täyttääkö yritys AEO-sertifikaatin vaatiman minimitason ja samalla tuoda tietoon tarvittavat parannukset.

Työssä on tarkoitus käydä läpi ensin pk-yrityksen tietoturvaa koskevaa lainsäädäntöä ja muita sitä ohjaavia yleisiä standardeja. Tarkoitus on selvittää yrityksen käytössä olevat työasemat ja palvelimet sekä kerätä käytössä olevat ohjelmistot ja käydä läpi niiden yleisimpiä riskejä.

Myös tietoturvaa ja yrityksen henkilöstöä käydään läpi sen verran, että saadaan tietää mahdollisen koulutuksen tarve ja vastuuhenkilöt. Lisäksi toteutetaan tietoturvakartoitus englanninkielisenä kyselynä, jotta AEO-sertifikaatin minimitasoa vaativa alihankkija voi olla mukana käsittelemässä tietoturvakartoituksen jälkeistä kehitys- ja koulutustyötä. Lisäksi käydään läpi AEO- sertifikaatin asettamat ohjeistukset ja minimivaatimukset yrityksen tietoturvalle.

# 1 MITÄ ON TIETOTURVA

Tietoturvalla tarkoitetaan yleisesti tiedon, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tavallisesti tietoturvalla on kolme päätavoitetta yrityksen toiminnassa: tiedon luottamuksellisuus, eheys ja saavutettavuus. Näiden toteutuminen yrityksessä vaatii hyvää suunnittelua. (Laakso 2013)

Luottamuksellisuuden tarkoitus on estää tiedon välittyminen ulkopuolisille. Kohde tulee suojata siten, ettei tietovuotoja pääse tapahtumaan missään tapauksessa. Eheys puolestaan tarkoittaa sitä, että tieto välittyy osapuolelta toiselle muuttumattomana. Tiedot tulee turvata, ettei niitä päästä muokkaamaan ilman asianmukaisia valtuuksia. Nämä kaksi tavoitetta voidaan täyttää yksinkertaisillakin teknisillä toimenpiteillä, kuten tiedon salaamisella (salasanat) tai tallentamalla tieto ulkoiselle medialle (dvd). Kun tieto on salattu tai tallennettu erillisille tiedostoille, voi sen saatavuus olla huono, koska tietoja joudutaan etsimään tai lataamaan eri paikoista, sekä se saattaa olla suojattu salasanoilla. Tämä korostaa hyvän suunnittelun ja menettelytapojen tarkoituksenmukaisuutta eli suunnitelmat pitäisi tehdä yksilöidyn tarpeen mukaisesti. (Laakso 2013)

Kiistämättömyys ja todentaminen voidaan lisätä tietoturvan tavoitteiksi. Niiden avulla voidaan varmistua, että tieto on asianmukaista ja oikeista lähteistä peräisin. Todentaminen on osa luottamuksellisuutta ja siksi yrityksellä tuleekin olla tietyt menettelytavat, joiden kautta voidaan varmistua järjestelmien käyttäjien henkilöllisyydestä. Valtuutettujen henkilöiden todennus voi tapahtua esimerkiksi tunnusta ja salasanaa käyttämällä. Muita mahdollisuuksia ovat sormenjälkitunnistimet, sähköiset avainkortit ja vaihtuvat koodit. (Laakso 2013)

Kiistämättömyys liittyy toiminnan todentamiseen, jonka avulla voidaan vähentää ja ehkäistä järjestelmien väärinkäyttöä. Käytännössä tämä tarkoittaa ohjelmistojen käyttötietojen tallentamista palvelun lokitiedostoihin. Tiedostoihin voidaan tallentaa tiedot ohjelmiston käyttäjästä, muutoksista ja ajasta, joiden tiedoista näkee, milloin muutokset on tehty. Lokitietojen turvaaminen mahdollisilta tietomurroilta

on ehdoton edellytys. Jos murto tapahtuu, niin luottamuksellisuus ja eheys kärsivät. Tietoa ei myöskään voi tällaisissa tapauksissa osoittaa kiistämättömäksi. Kaikki nämä viisi tietoturvan tavoitetta muodostavat yhdessä pohjan yrityksen tietoturvan rakentamiselle. (Laakso 2013)

### 1.1 Tietoturva yritysmaailmassa

Tietoturva on yritysmaailmassa liiketoiminnan tukemista ja tietojen suojaamista. Suojaaminen on perusteltua, koska tiedosta on tullut monelle yritykselle tärkeä osa menestymistä tiukentuvilla markkinoilla. Yrityksessä käytännön tasolla tietoturva on pieniä tekoja osana jokapäiväistä toimintaa. Kaikkien tulisi ymmärtää merkitys ja tavoitteet organisaatiotasolla, jotta haluttuihin tavoitteisiin päästäisiin. (Laaksonen, Nevasalo & Tomula 2006 17; Paavilainen 1998, 3)

Käytännössä näitä toimia ohjaa lainsäädäntö, joka antaa selviä sääntöjä, rajoitteita ja erilaisia kehitysvaatimuksia. Tämän perusteella täytyy yritysten tietoturvaa kehittää. Hyvä tietoturvan taso on yritykselle kilpailuetu ja se saattaa olla viimeinen vaikuttaja tiukassa tarjouskilpailussa, jossa on nykyään vaadittu esimerkiksi tietty taso tietoturvalle. (Laaksonen ym. 2006, 17)

Yritysten haasteet kilpailun voimistuessa ovat tietoturvan osalta antaa riittävästi resursseja tietoturvan ylläpitoon ja kehittämiseen. Se ei ole nykypäivänä itsestäänselvyys, kun suurin osa ajasta menee operatiivisten asioiden hoitamiseen. Yrityksen tietoresurssit saattavat olla nykypäivänä niin monessa eri paikassa ja vaikeasti havaittavissa. Tieto voi liittyä esimerkiksi toimintaan, asiakassuhteisiin tai organisaatioon. Esimerkiksi pelkästään tiedon sijainnin määrittely voi olla vaikeaa, koska tieto voi olla jakaantunut asiakirjoihin, cd-levyihin, levykkeisiin, sekä osa tiedosta voi olla ns. henkistä pääomaa työntekijöiden muistissa. Osa tiedosta voi olla organisaation toimintaan liittyvää ja se ei välttämättä ole missään tallenteessa vaan vain osalla ihmisiä. (Laaksonen ym. 2006, 19)

### 1.2 Lainsäädäntö ja vaatimukset

Yritykset toimivat nykypäivänä globaalissa ympäristössä ja toiminnassa tulisi huomioida kansainväliset lait ja asetukset. Tämä tarkoittaa Suomessa toimivalle

yritykselle käytännössä Euroopan unionin sisällä vallitsevia käytäntöjä. (Laaksonen ym. 2006, 23)

EU-lainsäädäntö on säätänyt monia välittömästi ja välillisesti tietoturvaa koskevia direktiivejä, joista osa on otettu käyttöön myös Suomen lainsäädännössä. Direktiivit eivät koske jäsenmaita ilman niiden kansallista vahvistamista, mutta osassa direktiivejä on välittömiä vaikutuksia myös ilman vahvistamista, jos kansallinen täytäntöönpanoaika on umpeutunut ja ne ovat ehdottomia ja riittävän tarkkoja. (Laaksonen ym. 2006, 26)

Kaksi ehkä tärkeintä direktiiviä tietoturvan kannalta ovat henkilötietojen suoja ja sähköisen viestinnän tietosuoja. Yrityksen tietoturvaa valvomaan tai määrittelemään ei ole laadittu Suomessa suoranaisia omia lakeja, joiden mukaan yrityksen täytyisi toimia. Käytännössä yrityksiä ohjaavat kuitenkin erilaiset lait, joista tulee olla tietoinen, koska yritys on käytännöntasolla itse vastuussa tietoturva-asioidensa hoitamisesta. (Laaksonen ym. 2006, 26)

Aikaisemmin yritys pystyi määrittämään tietoturvansa tason hyvin itsenäisesti, koska sellaisia yhtenäisiä säädöksiä, lakeja ja suosituksia, jotka suoraan ohjaisivat yrityksen tietoturvan tasoa ja ratkaisuja ei ollut niin paljon yhteiskunnan puolelta. Lakien lisäksi erilaiset vapaaehtoiset standardit ja sertifikaatit ovat lisänneet tietoturvatietoisuutta ja tuoneet lisää mahdollisuuksia vapaaehtoiseen tietoturvan kehittämiseen. Nämä ovat osaksi lisänneet myös yritysten painetta kiinnittää enemmän huomiota omaan toimintaansa ja sen kehittämiseen. (Laaksonen ym. 2006, 17)

Tietoyhteiskunnan kehittyessä nopeasti todettiin kuitenkin, että tarvitaan selkeitä lakeja ja ohjeita, että tietoturva pysyy tietotekniikan kehityksen mukana. Nykyinen kansallinen tietoturvastrategia pyrkii tasapuoliseen strategiaan, jossa huomioidaan kaikki aina yritysten reilusta kilpailuasemasta yksittäiseen ihmiseen. Siihen vaikuttavat kuitenkin yhteiskunnan puolelta erilaiset suorat ja epäsuorat lait ja ohjeistukset, jotka ohjaavat ja velvoittavat yrityksen toimia tietoturva-asioissa. (Laaksonen ym. 2006, 18)

Nykyiseen lainsäädäntöön on tullut enemmän ohjeistusta, kuinka tietoturvan eri vaiheita pitäisi toteuttaa ja määritystä on tarkennettu. Tietoturva on hyvin yksityiskohtaista käytännön tasolla, kun taas laki on enemmän yleistä ja enemmän tulkinnanvaraista. Näiden yhteensovittaminen tuo paljon uusia haasteita ja mahdollisuuksia tulevaisuudessa. Erillisestä tietoturvalaista on ollut laajaa keskustelua julkisuudessa. Sen tarpeellisuutta ei ilmeisesti ole pidetty riittävänä, vaan on katsottu, että nykyinen muu lainsäädäntö on riittävän kattavaa. Yritykset ovatkin alkaneet luopua osasta tietoturvaohjeita sekä erilaisia käytäntöjä ja ovat alkaneet integroida niitä osaksi muuta toimintapolitiikkaansa. (Laaksonen ym. 2006, 18, 21)

### 1.3 Liiketoiminnan tarpeet ja tietoturva

Yrityksen liiketoiminta nojaa yrityksissä nykyään hyvin vahvasti erilaisiin tietojärjestelmiin, jotka sisältävät tietoa aina asiakkaista omiin alihankkijoiden ja toimittajien tietoihin. Tietoa käsitellään ja sitä syntyy lisää päivittäin yrityksissä. Toiminta edellyttää kaiken tiedon olevan oikein ja ajan tasalla. Lisäksi tiedon tulee olla koko ajan saatavilla niille, jotka sitä työssään tarvitsevat. (Laaksonen ym. 2006, 19)

Nykyään yrityksissä on myös ulkopuolisia tekijöitä, jotka asettavat lisää vaatimuksia yrityksen tietoturvan tasoon. Yhä useammin hakkerit pääsevät käsiksi salaisiin tietoihin ja mitä suurempi yritys on, sitä kiinnostavampana se nähdään. Yritysten kansainvälistyessä myös maine ja markkinat odottavat täsmällistä tietoa ja esimerkiksi näiden luottamus saattaa olla jopa tärkeämpää kuin itse tietojärjestelmissä makaava tieto. Suuren pörssiyhtiön arvo saattaa laskea nopeasti, jos uutisoidaan tietomurroista ja sijoittajien luottamuksen palautumiseen voi mennä kauan. Myös investoinnit ja suuret omistajat haluavat salaisen tiedon pysyvän turvassa. (Laaksonen ym. 2006, 19)

Tiedon ollessa kiinteä osa koko liiketoimintaa se tarkoittaa sitä, että tietoturva on mukana koko yrityksen toimintaa. Tarvitaan koko henkilöstö mukaan huolehtimaan tietoturvasta, koska pelkästään fyysiset laitteet ja ohjelmat eivät riitä takaamaan tarvittavaa turvallisuuden tasoa. Tarvitaan myös hallinnollisen tietoturvan toimenpiteitä, joihin kuuluu määritellä tietoturvatoiminnan suuntaviivat ja erilaiset

turvallisuutta parantavat toimenpiteet. (Laaksonen ym. 2006, 19; Paavilainen 1998, 48)

Liiketoiminnan turvaamiseen liittyy kiinteänä osana myös hallinnollinen tietoturva. ”Hallinnollisen tietoturvan tehtävänä on määritellä, kuka vastaa turvallisuus-, toipumis-, ja valmiussuunnittelusta ja niihin kuuluvista toimenpiteistä. Siinä luodaan tyypillisesti seuraavanlaiset ohjeet

- Tietoturvasuunnitelma
- Toipumissuunnitelma
- Valmiussuunnitelma.

Tietoturvasuunnitelmalla määritellään ja toteutetaan perusturvallisuuteen liittyvät asiat. Se on hyvin tärkeä osa turvallisuutta, koska suurin osa vahingoista johtuu nimenomaan perusturvallisuuden laiminlyönneistä. Vahinkojen välttämiseksi tulee aina olla olemassa tietoturvasuunnitelma, jossa määritellään pahimmat uhat, ei toivotut tapahtumat sekä niiden jälkeiset toimenpiteet.

Toipumissuunnitelma pitää sisällään virheen jälkeiset korjaavat toimenpiteet. Toipuminen virheestä on tärkeä osa hallinnollista turvallisuutta mutta se unohtuu hyvin usein. Virheen jälkeen dokumentaation tulisi olla aukoton, että järjestelmä toipuisi virheestä mahdollisimman hyvin.

Atk- valmiussuunnitelma on poikkeusoloihin liittyvää suunnittelua. Tyypillisesti valmiussuunnitelma tehdään vain valtionhallinnossa ja yrityksissä, joissa on erittäin kriittisiä järjestelmiä.” (Paavilainen 1998, 49)

Yrityksen tulisikin keskittää toimintaansa pois teknispainotteisesta suuntautumisesta, koska tutkimusten mukaan hallinnollisella tietoturvaan panostamisella, mm. koulutuksella, voidaan saavuttaa huomattavia tuloksia tietoturvan kehittämisessä. Tärkeintä on, että yrityksen toiminnan kannalta tärkeimmät tiedot vastaisivat heidän harjoittamansa liiketoiminnan vaatimuksia. Lisäksi mahdollisiin poikkeamatilanteisiin varautumalla voidaan varmistaa se, ettei oikeassa tilanteessa jäädä vain

tuleen makaamaan, vaan henkilöstöllä on selkeät tavat toimia. Tällainen toiminta lisää luottamusta myös asiakkaiden keskuudessa.

# 2 LAITTEET JA TIETOTURVA

## 2.1 Fyysinen tietoturva

Fyysinen ympäristö tarkoittaa organisaation toimitiloja. Näiden tilojen suojaaminen luo koko yritykselle tietoturvan perustan. Tilojen suojaamisen suunnitteluun tarvitaan erilaisten turvallisuus- ja ratkaisuvaihtoehtojen selvitystä ja tutkimista. (Laaksonen ym. 2006, 125)

Korkeamman fyysisen suojauksen tiloja ovat organisaatiossa kaikki tilat, jossa toimitaan omilla vastuualueilla, kehitetään tuotteita, hallitaan atk-laitteita, sekä muut hallinnolliset tilat. Nämä kannattaa kuitenkin käydä läpi erillisessä riskikartoituksessa, että saadaan oikea kuva suojauksen tarpeesta. Myös korjausten suunnittelun yhteydessä on hyvä kirjata muistiin tilojen tarvittava suojaustaso ja mahdolliset puutteet, että niihin voidaan jo korjausaikana puuttua. (Laaksonen ym. 2006, 125)

Fyysiseen suojaamiseen liittyviä standardeja ovat esimerkiksi ISO 27001 standardi, joka sisältää omat vaatimukset tilojen suojaamiseen. Puolustusvoimilla on omat Vahti-ohjeistukset tilasuojaukseen ja Viestintävirastolla on oma ohjeistus suojauksesta fyysisten turvallisuusohjeiden mukaan. (Laaksonen ym. 2006, 125)

Toimitilojen suojauksessa pitäisi ottaa huomioon ainakin viisi eri kohtaa.

1. Varkaus

   Tietokonevarkaudet ovat koko ajan kasvava ongelma. Ne koskevat itse koneiden lisäksi myös muisteja, piirejä ja muita oheislaitteita. Ne sisältävät paljon tärkeää tietoa, joka ei saa joutua vääriin käsiin. Pääsy laitetilaan on estettävä ja myös työaikaisen liikkumisen kriittisissä tiloissa tulee olla valvottua.

2. Tulipalo ja lämpötilan liiallinen kohoaminen

   Jo pelkkä savu laitetiloissa voi vahingoittaa talletusmediaa. Tiloissa tulisikin huomioida hyvä ilmanvaihto ja lämpötila-anturit, ettei lämpötila pääse

esimerkiksi tulipalon seurauksena kohoamaan liikaa. Myös paloturvallisuusmääräysten mm. riittävien paloeristeiden, pitää olla kunnossa. Tulipalon aiheuttamiin vahinkoihin voidaan varautua mm. tärkeiden tietojen varmuuskopioinneilla.

3. Vesivahinko ja kosteus

   Jo laitetilan suunnittelussa tulisi huomioida, etteivät vesiputket ja viemärit mene tietotekniikkaa sisältävien tilojen luota voiden aiheuttaa esimerkiksi tallenteiden tai muiden kriittisten laitteiden rikkoutumista. Vahinkojen välttämiseksi voidaan harkita rakennettavaksi esimerkiksi erillinen välipohja, joka suojaa vesivahingoilta.

4. Sähköhäiriö

   Häiriöt sähkönsyötössä voivat aiheuttaa katkoksia ja rikkoontumisia. Laitteisto tulisi suojata ylijännitteiltä, virtapiikeiltä ja esimerkiksi ukkoselta suojaavien laitteiden avulla. Lisäksi pitää harkita UPS-laitteita ja mahdollisia varageneraattoreita. Työ ja koneet voivat kärsiä mittavia vahinkoja, jos laitteista on pitkään virta pois. Myös tietoa saattaa kadota.

5. Pöly

   Pölyä kertyy helposti atk-laitteisiin ja se tukkii helposti tuulettimet, sekä aiheuttaa tulipaloriskin. Laitteet tulee nostaa lattiatasosta, että pölyn kertyminen estettäisiin. Pöly voi rikkoa laitteita ja tallennusmediaa. Pölyn minimoimiseksi tulisi järjestää säännöllinen ja kunnollinen siivous kaikissa tiloissa. Pölyn kertymisen estämiseksi myös kaikissa laitetiloissa tulisi välttää turhaa kulkemista, että pölynmäärän voisi minimoida. (Laaksonen ym. 2006, 125)

## 2.2 Ohjelmistoturvallisuus

Yrityksen laitteistoturvallisuus käsittää käytössä olevan laitteiston ja sen käyttöjärjestelmät. Ohjelmistoturvallisuus puolestaan sisältää käytössä olevat sovellusohjelmat ja niiden toimivuuden yhdessä käyttöjärjestelmän kanssa. Eli käytännössä esimerkiksi, että yrityksessä käytössä oleva Windows 7-käyttöjärjestelmä toimii saumattomasti F-securen virustorjuntaohjelmiston kanssa, ettei tietovuotoja synny niiden yhteistoiminnassa.

Ohjelmistoturvallisuus voidaan tarkistaa esimerkiksi erillisellä tarkistuslistalla, joka käsittelee ohjelmistoja ja niiden luotettavuutta. Tähän liittyy useita näkökohtia, jotka yrityksen tietoturvavastaavan tulee huomioida Tärkeimmät huomioonotettavat asiat ohjelmistoturvallisuudesta on listattu alla:

- Käytettävien ohjelmien laatu

  Käytettyjen ohjelmien laillisuus eli lisenssit ja tietoturvaominaisuudet ovat hyvän tietoturvan pohja. Yritysten tulee varmistaa, että käytössä olevat ohjelmat ovat laillisia ja sitä kautta luotettavia ja toimivia. Piraattiversiot eivät tarjoa ylläpitoa tai /ohjelmistopäivityksiä, jotka varmistavat tietoturvan jatkuvan tason. Erilaiset lisenssisopimukset ja niiden voimassaolo takaavat myös ohjelmistojen toimintakyvyn ja työn ongelmattoman jatkumisen.

- Virustorjunta

  Viruksentorjuntaohjelmistoja käyttämällä voidaan estää erilaisten matojen, troijalaisten tai muiden haittaohjelmien pääsyä koneelle. Useimmiten virukset aiheuttavat vain koneen hidastumista, mutta pahimmassa tapauksessa ne kopioivat salaista tietoa koneelta.

- Ohjelmistojen pääsyvalvonta

  Pääsy ohjelmistoihin tulisi olla vain niillä, jotka sitä tarvitsevat. Näin voidaan välttyä turhilta tietovuodoilta ja parantaa ohjelmistoturvallisuutta. Pääsyvalvonta voidaan järjestää salasanoin tai muita tunnisteita käyttämäl-

lä. Tämä varmistaa, että vain oikeat henkilöt pääsevät käyttämään ohjelmistoja kirjautuessaan.

- Ohjelmistolokien ylläpito ja seuranta

  Laadukkaat ohjelmistot mahdollistavat tapahtumien kirjaamisen muistiin. Yrityksen tulisi jatkuvasti seurata, kuka ohjelmistoa käyttää ja mihin aikaan. Myös ongelmatilanteista lähtee tieto ylläpidolle, joka voi heti reagoida tilanteeseen.

- Alkuperäislevykkeiden ja varmuuskopioiden säilytys

  Ohjelmistojen alkuperäiset levykkeet ja varmuuskopiot tulee säilyttää lukitussa paikassa, että ne eivät pääse vääriin käsiin. Lisäksi ne tulee säilyttää eri paikassa mahdollisten murtojen tai katoamisien varalta. Varmuuskopioita tulee tehdä tarpeeksi usein, jotta tiedot ovat palautettavissa helposti ohjelmistojen häiriötilanteissa.

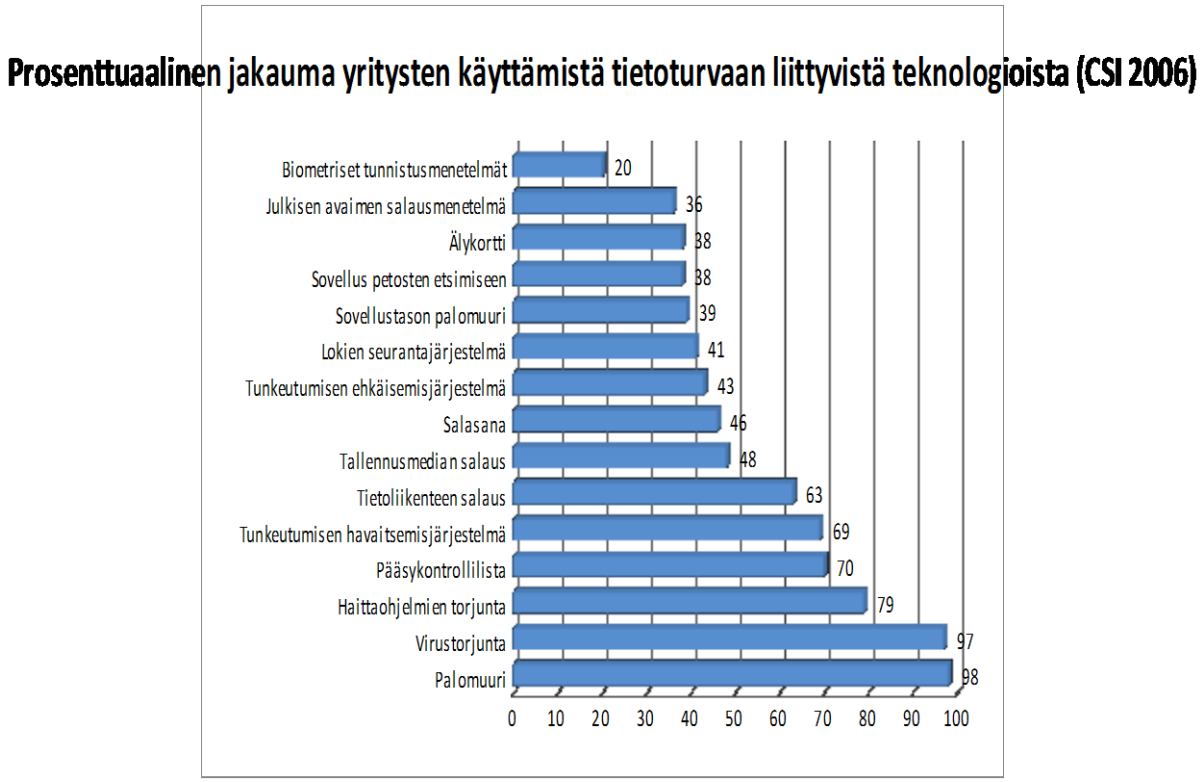
- Ylläpitosopimukset ja toimittajien vakavaraisuus

  Kun solmitaan ylläpitosopimuksia, tulee toimittajien ylläpitokyky tarkistaa. Näin voidaan varmistua siitä, että ohjelmistoja päivitetään jatkuvasti ja ne pystyvät tarjoamaan tulevaisuudessakin parhaan mahdollisen ohjelmistoturvallisuuden. Ylläpitosopimusten jatkuvuudesta on myös huolehdittava, ettei esimerkiksi viruksentorjunta yhtäkkiä poistu käytöstä ja aiheuta ohjelmistoturvallisuusriskiä. (Laakso 2013)

## 2.3 Työasema

Suomalaisissa yrityksissä työasemien virustorjunta on pääsääntöisesti hyvällä mallilla. Kuvassa 1 näkyy vuoden 2006 prosentuaalinen jakauma yritysten tietoturvalaitteistoista. Lähes jokaisella yrityksellä on käytössä palomuuri ja viruksentorjuntaohjelmisto. Henkilöstön tietoturvasta huolehtiminen on kuitenkin suoraan verrannollinen koulutuksen ja kunnollisten

ohjeiden määrään. Ohjeiden laatimisen lisäksi pitäisi tunnistaa yksilöidyt tarpeet ja tehdä ohjeet räätälöidysti yrityksen tarpeiden mukaan. (Laaksonen ym. 2006, 161, 204, 284)




**Kuva 1.** Vuoden 2006 prosentuaalinen jakauma yritysten tietoturvalaitteistoista. (Laaksonen ym. 2006, 284)

Erilaisia riskejä pk-yrityksen työpisteiden tietoturvaa ajatellen ovat:

1. Virukset

Selainten kautta tarttuvien virusten torjuntaan toimii yrityksessä parhaiten internetin käyttöä koskeva ohjeistus. Ensin pitää määritellä, mihin internetiä saa käyttää. Laki ei anna oikeutta seurata yksittäisen ihmisen käyttöä, mutta erilaiset rajoitukset esimerkiksi aikuisviihdesivuille saa ottaa käyttöön. Kaikki sopimaton käyttö on myös mahdollista rajoittaa sopimisella. (Laaksonen ym. 2006, 164)

Yleensä työntekijälle voidaan sallia esimerkiksi vähäinen yksityisten asioiden hoitoon kohdistuva käyttö. Tämä on silloin hyvä myös kertoa yleisessä ohjeistuksessa. Työntekijä on hyvä perehdyttää myös virusten ja haittaohjelmien tunnistamiseen, että mahdolliset riskit pystytään tunnistamaan. (Laaksonen ym. 2006, 163)

Selainten tietoturvaa voi parantaa esimerkiksi ohjaamalla kaikki liikenne tietyn proxyn kautta ja hoitamalla liikenteen tietoturva siinä keskitetysti. Näiden ulkoistuksessa on myös hyvä muistaa riittävä raportointi ja tarpeeksi kattava ohjeistus palvelun toimittajalle. (Laaksonen ym. 2006, 205)

Samat varotoimet ohjeistuksesta ja käytön määrittelystä pätevät myös sähköpostiliikenteeseen. Siellä ongelma on kuitenkin myös käyttäjästä riippumaton ns. roskaposti ja tietojenkalastelu eli phishing. Tämä tarkoittaa riskiä suoranaiseen tietojenkalasteluun tai koneelle latautuvaan haittaohjelmaan. Erilaisia roskapostisuodattimia koskeva lainsäädäntö on epäselvä, koska laki ei suoraan määrittele mitä kaikkea saa suodattaa, vaan laki kertoo seikkaperäisesti suodattamisesta ”välttämättömiä verkkopalvelujen tai viestipalvelujen taikka viestin vastaanottajan viestimahdollisuuksien turvaamiseksi.” Tämän lakitekstin johtopäätöksenä voitaisiin pitää, että suodatuksen aloittamisessa ja suunnittelussa olisi hyvä pyytää siihen myös työntekijän suostumus. (Laaksonen ym. 2006, 206)

2. Etä- ja kotikäyttö sekä omat tallennusmediat

Etä- ja kotikäyttö luovat uusia haasteita työpaikan työasemien virustorjunnan järjestämiseen. Tietoturvan nimissä tulisikin rajoittaa työntekijöiden henkilökohtaisten tallennusmedioiden liittämistä työasemille ja verkkoon. Tietoa ei missään vaiheessa saisi viedä tilaan, jossa tietoturva ei ole sen turvallisuuteen vaatiman tason mukaisesta säilytetty. Omat tallennusmediat saattavat myös altistaa yrityksen verkon alttiiksi viruksille ja muille riskeille. (Laaksonen ym. 2006, 204; Paavilainen 1998, 39)

3. Käyttöoikeudet ja tiedon suojaaminen

Suojaamattomalle työasemalle pääsy on merkittävä tietoturvariski. Salasana on yksinkertaisin tapa suojata työasemalle pääsy. Tämän takia yrityksessä on hyvä määritellä käytännesäännöt eli tehdään erittely käyttöoikeuksista eri tiedostoihin. Oikein jaetut käyttöoikeudet poissulkevat ongelmia mm. ylimääräisistä salasanoista, kun käyttöoikeudet on jaettu työasemakohtaisesti. (Laaksonen ym. 2006, 174,146)

Tietojärjestelmien ja ohjelmien käyttöoikeudet tulisi määritellä selvästi kahteen osaan:

- Järjestelmän ylläpitäjän tunnukset
- Järjestelmän käyttäjän tunnukset

Tällä minimoidaan tiedon muuttumattomuus ja virhetilanteet. (Laaksonen ym. 2006, 176; Paavilainen 1998, 38,39)

4. Käyttöönotto ja ohjeistus

Henkilöstö on pääosassa torjuttaessa tietoturvaan liittyviä riskejä. Henkilöstöä on jatkuvasti koulutettava, että tietoturvan hallinta olisi riittävällä tasolla. Tämä tarkoittaa työntekijän koko työssäoloaikaa. Se tarkoittaa riittäviä suunniteltuja standarditoimenpiteitä aina rekrytoinnista henkilön työsuhteen loppumisen jälkeen. (Paavilainen 1998, 91,93)

Omien kokemuksieni perusteella pienessä pk-yrityksessä erilaisten atk-laitteiden käyttöönotto ja asennus saatetaan suorittaa itse paikan päällä. Pienessä yrityksessä ei olla aina selvillä siitä, kuka on vastuussa ja kenellä on tarvittava tietotaito tietoturvaa käsittelevien tehtävien hoitamiseksi. Riskin minimointi vaatii standardoituja asennus ja käyttö-ohjeita. Lisäksi tulisi tarvittaessa henkilökuntaa kouluttaa tehtävien vaatimalla tavalla. Näiden avulla asennuksessa ja käyttöönotossa voitaisiin varmistua vaaditusta tietoturvatasosta. Riittävien vaatimusten listaaminen yleisohjeeksi asennukselle ja käyttöönotolle pitäisi tehdä ja liittää osaksi tietoturvan käyttöopasta. (Laaksonen ym. 2006, 215)

5. Järjestelmän auditointi

Järjestelmän muuttuvat vaatimukset edellyttävät jonkin asteista auditointia. Sen tulisi olla mielellään säännöllistä ja siinä tulisi ottaa huomioon muuttuneet vaatimukset sekä uudet määräykset. Yksinkertaisia järjestelmiä voi auditoida manuaalisesti, koska niiden tieto on vielä helposti hallittavissa. (Laaksonen ym. 2006, 216)

Suurempien ja monimutkaisten järjestelmien osalta voidaan käyttää erilaisia automaattisia ohjelmia ja järjestelmiä esimerkiksi auditointiskriptiä. Järjestelmää tulisi auditoida aina myös verkon näkökulmasta ja ulkopuolisia uhkia vastaan. Automaattiset skannerit, esimerkiksi ISS Internet Scanner voivat etsiä mm. verkon haavoittuvuuksia. Symantec Enterprise Security Manager on työkalu, joka etsii puutteita esimerkiksi tietoturvapäivityksistä, heikoista salasanoista, tiedosto-oikeuksista ja raportoi myös erilaisista standardien vastaisista tietoturva-asetuksista. (Laaksonen ym. 2006, 216)

Automaattisen skannerin toimintaa kuvaa työasemille esimerkiksi secunian tarjoama OSI eli Online Software Inspector ohjelmaa. Ohjelma käy läpi työaseman systeemiin ja ohjelmistoon liittyvät asiat aina päivityspaketeista uusimpiin versioihin ja antaa automaattisesti korjaus tai päivityskehoituksen. Skannaus kestää noin viisi minuuttia ja antaa nopeasti pintapuolisen tiedon siitä onko kaikki kunnossa. Saman valmistajan ohjelmistoja käyttää esimerkiksi Siemens. Samalla toimintaperiaatteella toimivat myös monimutkaisemmat ja maksulliset skannerit esimerkiksi ISS Internet Scanner.

Riippuen yrityksen koosta kannattaa harkita, onko auditointi ulkopuolinen vai suoritetaanko se yrityksessä itsenäisesti. Suuremmalle yritykselle sopii paremmin ulkopuolinen auditointi, koska se ei sido yrityksen omaa organisaatiota ja on yleensä tehokkaammin toteutettu. Ulkopuolisella yrityksellä on yleensä valmiit standardit ja se voi esimerkiksi tarjota määräajoin ajettavia säännöllisiä raportteja.

Ulkopuolisen auditoijan kautta on myös mahdollisuus saada yrityksen järjestelmälle sertifikaatti, joka toimii todistuksena standardin mukaisen järjestelmästä. (Laaksonen ym. 2006, 217)

Opinnäytetyössäni toteutin pk-yritykselle tietoturvakartoituksen, joka toimii järjestelmän auditointina. Näin saatiin lähtökohdat tietoturvatasolle. Liitteessä 1 on tietoturvakartoitukseen käytetty lomake.

Työpisteiden tietoturvariskejä ajatellen pk-yrityksessä oli huomioitu joitakin perusasioita jo nykyisessä toiminnassa. Työkoneilla oli viruksentorjuntaohjelmat, etäkäyttöä ei juuri ollut, joten sitä ei voitu pitää varsinaisena riskinä, käyttöoikeudet salassa pidettävään materiaaliin oli vain niillä, jotka sitä tarvitsivat ja materiaaliin pääsi käsiksi salasanan ja käyttäjätunnuksen avulla. Yrityksellä ei ollut selkeitä toimintaohjeita, eikä käytäntöjä turvallisuusasioista. Eri käytännöt aiheuttavat turhaa sekaannusta ja vaaratilanteita tietoturvaa ajatellen. Työssäni laadin yhteiset pelisäännöt tietokoneiden käyttäjille tietoturvan parantamiseksi.

## 2.4 Palvelimen tietoturva

Työasemien virusturva verkossa ei yksin riitä. Myös palvelin tarvitsee oman tietoturvan. Yleensä se hoidetaan ohjelmallisesti. Palvelimen tietoturvaan liittyy aina samat riskit kuin myös muihin verkkoon liittyviin laitteisiin. Palvelimen tietoturva tulee ottaa esille jo tarjouskyselyvaiheessa, kun sen hankintaa aletaan suunnitella. Virustorjunnan asentaminen jälkeenpäin saattaa olla hankalaa, koska toimittaja ei välttämättä hyväksy muutoksia sopimukseen. Myös asentaminen voi olla työläämpää jälkikäteen. (Laaksonen ym. 2006, 204)

Palvelin on yrityksen kannalta hyvin kriittinen laite varsinkin dataa ja sisäverkkoa ajatellen. Tutkimusten mukaan yrityksen sisäverkon kaatuminen hidastaa merkittävästi operatiivista toimintaa ja sen lisäksi tiedonkulku katkeaa kokonaan. Tällaisessa tilanteessa voi arvokasta tietoa myös kadota, jos sitä ei ole ehditty tallentaa. (Paavilainen 1998, 146)

Suurimmat riskit sisäverkon ulkopuolelta palvelimelle ovat internetistä tulevat virukset ja erilaiset murtautumisyritykset. Niitä vastaan voidaan suojautua virus-

torjuntaohjelmilla ja palomuurilla. Myös erilaiset muut liikennöintirajoitukset, salasanat ja riskianalyysit ennen verkkoon menoa pienentävät riskejä huomattavasti. Palvelimelle murtautumisen havaitsemiseen tarvitaan kuitenkin käytännössä aina jonkinlaista tietoverkon valvontaa. (Laaksonen ym. 2006, 186,188; Paavilainen 1998, 144)

Palvelimen varmuuskopio on kriittinen ja yksi tärkeimmistä osista tietoturvaa. Jokaisen yrityksen tulisi ylläpitää varmuuskopioita tärkeistä tiedoista riskien välttämiseksi. Näin voidaan varautua mm. varkauksiin, tulipaloihin ja tietokoneiden oikosulkuihin.

Pk-yrityksessä, johon tietoturvakartoitus toteutettiin, kaikkien työasemien tiedoista ja yhteisistä tiedostoista otettiin varmuuskopiot palvelimelle ja varmuuskopio lähti myös verkon yli ulkopuoliseen konesaliin. Varmuuskopio meni ”Kasvavan vedostuksen menetelmällä” eli kaikki tieto kopioitiin kerralla varmuuskopioon ja sen jälkeen vain päivittynyt tieto lisättiin varmuuskopioon. Käytännössä tämä tapahtuu niin, että palvelimella olevaa muuttunutta tietoa verrataan verkkoasemalla olevaan varmuuskopiota sisältävään tietoon. Tämän jälkeen kaikki muuttunut tieto kopioidaan varmuuskopiolle. Tämä poistaa turhaa siirtämistä, koska muuttumatonta tietoa ei tarvitse siirtää uudelleen varmuuskopioon. Päivän päätteeksi klo 23.00 varmuuskopio lähti netin kautta ulkoiselle konesalille varmuuskopioksi. Tästä tuli heti soitto konesalilta, jos tuli jokin virhe tai tieto ei siirtynyt. (Paavilainen 1998, 222)

Pk-yrityksessä johon tein selvityksen it-laitteistosta oli palvelimen palomuuriratkaisu ostettu suoraan laitetoimittajalta ja heidän ylläpitonsa seurasi palvelimen epäilyttävää verkkoliikennettä. Laitetoimittajan oma ylläpito sai suoraan raportin palvelimen toiminnasta ja vahvistuksen jokapäiväisestä varmuuskopion siirtymisestä verkon yli. Jos johonkin tuli häiriö, niin siitä raportoitiin heti yritykselle. (Paavilainen 1998, 221)

# 3 HENKILÖSTÖ JA TIETOTURVA

## 3.1 Henkilöturvallisuus

Henkilöturvallisuudesta puhuttaessa tarkoitetaan henkilöstön tieturvan hallintaa. Henkilöturvallisuuden riskit luovat mahdollisuuden tahattomiin ja tahallisiin vahinkoihin, joita voidaan aiheuttaa. Myös henkilön tahallaan aiheuttamia vahinkoja voidaan pitää hyvin merkittävinä riskeinä. (Paavilainen 1998, 89)

Tietoturvan kannalta on tärkeää, että henkilöstö tunnetaan ja mahdolliset riskit minimoidaan aina rekrytoinnista työntekijän yrityksestä lähtemiseen saakka. Koulutus ja toimenkuva ovat luotava sellaiseksi, että se vastaa oikeasti yrityksen tarpeita. (Paavilainen 1998, 92, 94)

Rekrytoinneissa on mahdollista käyttää erilaisia psykologisia arviointeja ja poliisilta tilattavia turvallisuusselvityksiä. Myös työntekijöiden aiempi työhistoria ja yhteydenotot aiempiin työnantajiin mahdollistavat taustatiedon hankinnan. Tämä auttaa minimoimaan riskiä rekrytoinnissa. (Paavilainen 1998, 92)

Tietoturva on hyvin riippuvainen oman henkilöstön tekemisistä. Varsinkin pienessä pk-yrityksessä tietotaidon keskittyminen yhdelle tai vain muutamalle henkilölle on suuri riski. Tällaisessa tilanteessa täytyisi pitää vähintään kahden henkilön osaamista yllä ns. seuraajasuunnittelulla ja sijaistoiminnalla. Myös ilman vastuunjakoa saattaa yhden henkilön vastuu ja työtaakka kertyä helposti liian suureksi. Avainhenkilöille tulisi aina nimetä ja pitää ajan tasalla riittävän monta varahenkilöä, että mahdollinen työtaakan jakaminen ja tärkeä tietotaito ei olisi uhattuna. (Paavilainen 1998, 89,90)

Henkilön ominaisuudet eri tilanteissa tulisi pystyä tunnistamaan. Kaikki toimivat eri tavalla erilaisissa tilanteissa, ja varsinkin kiire sekä erilaiset stressitilanteet voivat luoda tietoturvariskejä, jos henkilö kaatuu paineen alla. Tällaiset paniikinomaiset ratkaisut ja muu liiaksi kasaantuneen paineen riski pitäisi pystyä minimoimaan riittävällä koulutuksella ja riskien tunnistamisella. Riski ja virhetilanteisiin koulutettu henkilö ei hätiköi hätätilanteessa, vaan pystyy toimimaan pa-

remmin, kun tällaiset uhkatilanteet on käyty koulutuksessa läpi. (Paavilainen 1998, 91)

Henkilön yrityksestä lähtemisen mukana siirtyy aina jonkin verran tietoa pois yrityksestä. Jos tulevassa työpaikassa työntekijä voi hyödyntää lähtevää tietoa, on hyvä tehdä sopimus liittyen salatun tiedon salassapitoon. Henkilön toimiminen samalla toimialalla voidaan kieltää työehtosopimuksen huomautuksella esimerkiksi viideksi vuodeksi. Kriittisen henkilön irtisanominen on aina riski ja yleensä työntekijälle irtisanomisilmoitus halutaan tehdä vasta viime tipassa että voidaan minimoida vuotavan tiedon mahdollisuus. Mahdollisten tietovuoto ja kostotoimenpiteiden minimoimiseksi voidaan käyttää esimerkiksi kultaista kädenpuristusta harkinnan mukaan. Myös irtisanomismenettelyllä on merkitystä irtisanottavan mielikuvaan edellisestä työnantajasta. Asiallisesti tehty irtisanominen jättää edes jokseenkin tyydyttävän kuvan yrityksestä ja vähentää kostonhalua. (Paavilainen 1998, 93)

Henkilön lähdettyä yrityksestä on hyvä käydä läpi, että hänellä ei ole enää pääsyä järjestelmään, ei avaimia tai muuta työpaikalle kuuluvaa. Tällaiset voisivat muuten mahdollistaa helposti väärinkäytöksiä tai tietomurtoja. (Paavilainen 1998, 93)

### 3.2 Tietoturvaohjeistus ja dokumentaatio

Yleensä tietoturvaohjeet laaditaan jonkun mallin tai standardin mukaan. Ohjeita laadittaessa tulee olla selkeä kuva, mitä oikeasti halutaan ja mikä on tarpeellista. Ohjeita tarvitaan aina ohjelmien käytöstä vierailutoimenpiteisiin ja netin käyttöön. On myös tärkeä huomioida eritasoiset käyttäjät. Nykyään nuorilla on yleisesti ottaen hyvä ammattitaito liittyen tietokoneisiin ja internetin käyttöön, mutta riippuen henkilöstä tietotaidot voivat vaihdella ikään tai sukupuoleen katsomatta huimastikin. (Laaksonen ym. 2006, 145,146)

Yrityksen tietoturvapolitiikka on ohjeita laajempi kokonaisuus. Se on ikään kuin tietty tila, jota halutaan ylläpitää, ja se pitää sisällään kaikki yrityksen tietoturvan aina koulutuksesta yleisiin linjauksiin asti. Tietoturvapolitiikka luo odotukset ja

vaatimuksen yrityksen tietoturvatoiminnalle, näin ollen sen tulee kuvata yrityksen todellista tietoturvatasoa. (Laaksonen ym. 2006, 146)

Ohjeistus on enemmän johonkin tiettyyn asiaan suunnattu ja tiettyä asiaa varten tehty ja jokapäiväistä toimintaa koskeva. Se voi kertoa esimerkiksi pelkästään yrityksen järjestelmien käytöstä. Pienelle pk-yritykselle olisi mielestäni tärkeää saada tietoturvaa koskeva yleisohje, koska yrityksen tietoturvaa ylläpidetään enemmän ulkopuolisesti. Ohjeessa tulisi käydä läpi mahdolliset käyttäjien kohtaamat riskit ja luoda niille selvä ohjeistus. Myös tietoturvan tärkeyden korostaminen motivoi henkilöstöä toimimaan huolellisesti tietoturvaa koskevissa asioissa. Tietoturvapolitiikka voisi siten tulla osaksi yrityksen laatujärjestelmää ja ohjeet voisivat olla esillä kaikille työntekijöille. (Laaksonen ym. 2006, 146)

Toimintaohjeissa tulisi luoda yritykselle tietty malli ja tapa hoitaa tietyt tietoturvaasiat. Sen pohjaksi voisi käydä läpi todelliset päivittäiset tilanteet, joihin tarvittaisiin tiettyä tapaa toimia. Ohjeisiin tulee sisällyttää, mitä tietyn toimenpiteen tietoturvan vuoksi pitää tehdä ja miten se tehdään. Pieneen yritykseen integroitu päivittäisten ohjeiden lista poistaisi turhia päällekkäisyyksiä ja se olisi varmasti tuloksellisin tapa toimia. Toimintaohjeet ja politiikka on hyvä kirjata toimintaohjeisiin, että niitä tarvitsevat henkilöt todella saavat tiedon ja ymmärtävät, mitä heidän tulee tehdä ja miksi. (Laaksonen ym. 2006, 146)

### 3.3 Pk-yrityksen tietoturvaohje

Laadin yrityksen toivomuksesta yksinkertaiset toimintaohjeet kaikille työpisteille. Halusin ottaa ohjeiden laatimisessa huomioon työntekijöiden tietotason ja halusin ohjeiden liittyvän päivittäiseen tekemiseen.

Käytin ohjeiden laatimisen apuna tietoturvakartoituksen teoriaa, yritykselle tekemääni laitteisto- ja ohjelmistokartoitusta, tietoturvakyselyä sekä Mikrosoftin ”10 tapaa työskennellä tuvallisemmin”- ohjetta. Mikrosoftin ohjeet antoivat hyvän pohjan työlle, koska työasemien ohjelmat ovat pääsääntöisesti heidän toimittamiaan.

Halusin valita ohjeisiin mielestäni viisi tärkeintä kohtaa, jotka mahdollistaisivat neuvoja päivittäisiin työtilanteisiin ja jotka ovat mielestäni nousseet esiin tätä prosessia läpikäydessä. Valmiit tietoturvaohjeet ovat liitteessä 1.

# 4 AEO-SERTIFIKAATTI JA TIETOTURVA

## 4.1 AEO-sertifikaatti yleisesti

Maailman tullijärjestö WCO laati vuonna 2005 AEO-standardin helpottamaan maailmanlaajuista kaupankäyntiä ja turvallisuutta. Tarkoitus on suojata kuljetettavaa tavaraa ja tietoa sekä helpottaa siihen sitoutuneiden tahojen kansainvälistä kauppaa erilaisilla tavaran vientiin liittyvillä helpotuksilla. Sertifikaatti kiinnostaa erityisesti yrityksiä, joilla on tuontia, vientiä ja tullattavaa, sekä niiden yhteydessä toimivia yrityksiä. (Tullihallitus 2013)

AEO-todistuksia on kolmea erilaista tyyppiä ja ne eroavat toisistaan niin vaatimuksiltaan kuin eduiltaan. Sertifikaatin kolme tyyppiä ovat:

- AEOC (Customs Simplifications, yksinkertaistetut menettelyt)
- AEOS (Safety and Security, vaarattomuus ja turvallisuus)
- AEOF (Full, yksinkertaistetut menettelyt sekä vaarattomuus ja turvallisuus) (Tullihallitus 2013)

AEOC on käytännössä toimijoille, jotka tarvitsevat helpotuksia tai nopeutusta tullauksessa yleisesti käytettäviin yksinkertaisiin tullimenettelyihin. Toimijan hakemusaikoja nopeutetaan ja tiettyjen lupien hakua nopeutetaan. Tämä on tarkoitettu ensisijaisesti vain Euroopan yhteisön alueella toimiville yrityksille. (Tullihallitus 2013)

AEOS on toimijoille, jotka vievät tai tuovat tavaraa laajemmin ulos Euroopan yhteisön alueelta ja jotka haluavat helpotuksia esimerkiksi tullauksessa ja tavaran tarkastuksessa. Tullitarkastuksessa saadaan helpotuksia ja jos tullitarkastuksiin joutuu tavaraa, niin siitä ilmoitetaan hyvin, että tällaiseen osataan varautua ja viivytyksiä ei syntyisi. Helpotuksia syntyy myös yleisilmoitusvaiheen tietojen antamisessa ja tulevaisuudessa AEO-toimijoiden ketjun vuorovaikutus voi antaa muitakin helpotuksia. Tällainen toimija ei käytä yksinkertaista menettelyä. Tämä taso

on myös yhteisön ulkopuolisille tahoille esimerkiksi varustamot ja lentoyhtiöt yhteisön ulkopuolelta. (Tullihallitus 2013)

AEOF on toimijoille, jotka ovat kiinnostuneita kaikista AEO-toiminnan eduista ja saattavat niitä tarvita, kuten toimitusketjujen turvallisuuden edistämisestä, yksinkertaistettujen tullimenettelyjen käyttämisestä, sekä helpotuksista tulli- ja yleisilmoitusvaiheen tarkastuksiin. Tämä taso on kaikille toimijoille, jotka ovat kiinnostuneet näistä helpotuksista. (Tullihallitus 2013)

Hakeutuminen AEO-toimijaksi edellyttää ensin perehtymistä AEO-toimijan vaatimuksiin ja säädöksiin. Tullihallitukselle tehdään hakemus ja täytetään alustava itsearviointi. Kun yritys on mielestään tehnyt ja täyttää kaikki AEO-kohdat, jotka yleensä vaativat selvitysvaiheessa esimerkiksi tullin tai ulkopuolisen konsultin apua, niin tullilta tilataan tarkastus ja selvitetään, täyttyvätkö vaatimukset. Jos vaatimukset täyttyvät heti tai vaadittavien korjausten jälkeen, voidaan yritykselle myöntää sertifikaatti. Hakuprosessiin on varattava aikaa kaikkine toimintoineen noin 120 + 60 päivää eli koko prosessi vie noin puoli vuotta.

Standardit täyttäneelle yritykselle myönnetään AEO-sertifikaatti. Sertifikaatin vaatimia toimenpiteitä ovat:

1. Tullivaatimusten noudattaminen toiminnassa
2. Taloudellinen vakavaraisuus
3. Riittävä logistiikka ja kirjanpitojärjestelmä
4. Käytössä riittävät turvallisuusnormit

Hakuprosessin aikana korostetaan auditointia ja fyysisiä käyntejä hakeutuvan yrityksen tiloissa eli vaatimukset ja toimenpiteet käydään läpi myös käytännön tasolla. (Tullihallitus 2013)

Tyypillisimpiä AEO-toimijoita EUn alueella ovat esimerkiksi tavaran valmistukseen, vientiin, tuontiin, tullaukseen, varastointiin, tullitoimintaan tai huolintaan erikoistuneet yritykset. Kaikki toimijat yleensä hyötyvät helpotetuista tullitoimin-

noista tai luotettavan toimijan maineesta joko suoraan tai esimerkiksi alihankkijan roolissa. (Tullihallitus 2013)

Ketjun tavoitteena on olla mahdollisimman kattava, koska esimerkiksi tavaran viennissä kaikki ketjuun osallistuvat tahot ovat omalta osaltaan vaikuttamassa tavaran ja tiedon turvallisuuteen. (Tullihallitus 2013)

Alihankkijana toimivan pk-yrityksen ei ole välttämätöntä hakea omaa AEO-sertifikaattia mutta yleisenä käytäntönä on, että asiakasyritys auditoi ja varmistaa koko toimitusketjun toiminnan olevan AEO-standardin mukaista. Tämä luo pk-yritykselle hyvän mahdollisuuden olla mukana hakemassa kasvua kokoajan globalisoituvassa teollisuudessa. Töitä saavat ne, jotka osaavat muuntautua tarpeille sopiviksi toimijoiksi. (Tullihallitus 2013)

Kyseisessä yrityksessä, johon lopputyö toteutettiin, pyrkimyksenä on täyttää asiakasyrityksen vaatimukset liittyen heille myönnettävään AEO-todistukseen. Yrityksessä on tehty alkuaudiointi ja tietoturvaselvitykseni nojaa osaksi siellä ilmitulleisiin vaatimuksiin ja parannustarpeisiin.

### 4.2 AEO ja tietoturvavaatimukset

AEO-todistus painottaa hakijaltaan tiedon ja fyysisen toimitusketjun suojaamista. Riskilähtöinen lähestymistapa korostuu, kun jokaista hakeutuvaa yritystä ja sen ketjua arvioidaan sen todellisen toiminnan asettamien riskien mukaan. (Tullihallitus 2013)

Tietoturvavaatimukset lähtevät siitä, että ensin tunnistetaan koko toimitusketjun toimijat ja riskit. Kuvassa 2 on lueteltuna AEO-turvallisuuden eri osa-alueet. AEO-sertifikaatti ei aseta selkeitä vaatimuksia, vaan pyrkii ohjaamaan yritystä omien tietoturvariskiensä arvioimiseen. Jokaisen yrityksen riskit ovat erilaisia, riippuen toimintatavoista ja menettelyistä, näin ollen yksityiskohtaisia ohjeita ei voida antaa.

Toimitusketjut voivat olla hyvinkin monimutkaisia, jos tuotteeseen liittyy useita alihankkijoita. Toimitusketju alkaa siitä, kun alihankkijalta tilataan tuote tai suun-

nittelutyö. Tämän jälkeen tuote tai tilattu tieto on kuljetettava suojattuna alihankkijalta tilaajalle. Tilaaja voi käyttää tuotteen itse tai se lähtee eteenpäin hänen asiakkaalleen. Toimitusketjun monimutkaisuus lisää riskejä ja siksi ison kansainvälisen yrityksen hankkima AEO-sertifikaatti asettaa vaatimuksia myös sen alihankkijoille. Vaikka alihankkijayritys on vain yksi osa toimintaketjua, mutta se on merkittävässä roolissa aiheuttaen riskin koko toimitusketjulle.

Yrityksen riskien arviointi liittyy omaan toimintaan, tiedonvälitykseen ja menettelyihin. Merkittävässä roolissa ovat alihankkijan omat alihankkijat, heidän tietoturvatasonsa arvioiminen, heille asetetut vaatimukset sekä oman toiminnan kriittinen arviointi. Tärkeintä on, että yritys on tietoinen omasta ja omien alihankkijoidensa tietoturvatasosta, arvioinut siihen liittyvät riskit ja pyrkii kehittämään toimintaansa jatkuvasti riskien vähentämiseksi. Valvonta on myös osa riskienhallintaa.

Kun riskit on arvioitu, voidaan toimitusketjua pyrkiä suojaamaan tarvittavin menettelyin. Mahdollisia menettelyitä ovat sidosryhmien taustojen tarkistaminen internetin tai luokituslaitoksen tietokantaa hyödyntäen ja erilaisten turvallisuusvaatimusten lisääminen sopimuksiin koskien tavaroiden pakkaamista, läpivalaisua, merkintöjä ja sinetöintiä. Lisäksi alihankkijoille voidaan asettaa tiukempia vaatimuksia yhteistyön jatkamiseksi tarkentamalla turvallisuusvaatimuksia, vaatimalla turvallisuusstandardin sertifiointia tai velvoittamalla heitä ilmoittamaan omista tietoturvariskeistä.

Tutkimassani yrityksessä on paljon kriittistä asiakasyrityksen tietoa fyysisesti ja paperilla, koska siellä pakataan ja lähetetään tavaraa eteenpäin. Suurimmat uhkakuvat alustavan auditoinnin perusteella olivat pääsy salaisiin asiakirjoihin ja fyysisesti laatikoihin sekä lähetystietoihin. Yleiseksi käsitykseksi pk-yrityksen AEO-vaatimuksissa muodostui yleisten tietoturvastandardien ja tietoturvakäytäntöjen mukainen toiminta.


**Kuva 2.** AEOS -vaatimukset. (Tullihallitus 2013)

# 5 PK-YRITYKSEN TIETOTURVAKARTOITUS

Kesällä 2012 asiakasyritys piti alustavan auditoinnin koskien pk-yrityksen tietoturvaa ja yleistä turvallisuustasoa yrityksen tiloissa. Tarkoituksena oli selvittää yrityksen tietoturvan nykytaso, sekä yleisellä tasolla käydä läpi täyttyykö AEO-sertifikaatin vaatima toimitusketjun turvallisuus alihankkijatasolla.

Pk-yrityksen kautta kulki ison asiakkaan arvokasta tavaraa, jonka suojaaminen oli erityisen tärkeää. Kriittistä oli suojata fyysisesti kaikki tavara riskeiltä, kuten esimerkiksi sabotoinnit, varkaudet ja terrorismi. Tietotekniset haasteet asetti tavarankulun mukana tuoma tiedonkulun suojauksen tarve. Tavaran mukana meni tietoa, esimerkiksi piirustuksia, manuaaleja, lähetystietoa, työohjeita ja muuta tietoliikennerikollisuuden vaaran piiriin kuuluvaa tietoa.

Tämän takia yritys tilasi minulta tietoturvakartoituksen ja pyysi selvittämään yleisesti AEO-sertifikaatin tuomia vaatimuksia tietoturvassa ja jokapäiväisessä toiminnassa. Myös yleisimmistä toimintamalleista tiedon suojaamiselle ja turvaamiselle haluttiin saada esimerkkejä ja teoriaa, että niiden avulla päästäisiin paremmin kehittämään omaa toimintaa.

Tietoturvasuunnitelman piirissä tulisi olla kaikki tilat, joissa yritys harjoittaa toimintaansa, että pystytään arvioimaan eri tilojen suojausten tarve. Ilman selvityksiä saattavat korkeaa suojausta tarvitsevat tilat jäädä vähemmälle suojaukselle ja vähemmän tärkeiden tilojen liiallinen suojaus syö resursseja tärkeämmiltä tiloilta. (Laaksonen ym. 2006, 125)

Tietoturvakartoituksen kautta pyrittiin tarkentamaan ja selvittämään riskit, jotka liittyivät yrityksen tietoturvaan sekä toimintamalleihin. Piti löytää helppo tapa kyseenalaistaa toimintamallit ja selvittää, ovatko kriittiset asiat tiedossa.

Kysymyslista, jolla yrityksen tietoturvan taso käytiin läpi, on liitteenä kaksi. Kysymyslistan tarkoituksena oli kerätä lyhyillä lauseilla vastauksia kysymyksiin ja lopuksi painottaa juuri niitä asioita, jotka olivat kyseisen yrityksen kohdalla tärkeitä ja joihin en ollut mielestäni saanut luotua kuvaa, miten ne asiat yrityksessä

on toteutettu ja miten niitä tulisi kehittää. Tarkoitus oli käydä läpi tietoturva aina lainsäädännöstä henkilöstöön ja laitteisiin.

Lyhyisiin vastauksiin päädyttiin myös, koska yrityksellä oli poikkeuksellisen paljon tilauskantaa ja käytännön syistä vastauksien miettiminen ja paperille saaminen piti hoitaa aina lyhyissä pikapalavereissa. Kartoitukseen löytyi hyvä pohja, joka piti sisällään tärkeimmät kohdat kokonaisvaltaisesta tietoturvan hallinnasta. Se oli riittävän yksinkertainen pienellä pk-yrityksellä ja siinä käytiin läpi tietoturva aina lainsäädännöstä henkilöstöön ja laitteisiin.

Tietoturvakartoitus toteutettiin joulukuussa 2012 käymällä läpi AEO-vaatimuksia ja sen jälkeen käymällä koko kyselylista läpi. Kyselyn jälkeen vastaukset kirjattiin muistiin ja niistä poimittiin kymmenen kriittisintä kohtaa, jotka olivat nousseet mielestämme pääkohdiksi alkuauditoinnissa kesällä. Jokaisen kysymyksen kohdalla vastausta yritettiin peilata yrityksen omaan toimintaan ja vastaavat riskit löytää asiakasyrityksen AEO-toimitusketjusta.

Yritys ei halunnut saada vastaukseksi mitään teoreettista opusta, vaan selkeät esimerkit siitä, miten heidän pitäisi käytännössä omia asioitaan parantaa. Tämä onnistuisi helpommin kiireen keskellä, eikä vaatisi välttämättä ulkopuolisia resursseja. Myös lopullinen AEO-turvallisuusvaatimus oli vielä auki ja haluttiin odottaa asiakasyrityksen uutta auditointia, että saataisiin varmuus tarpeellisille investoinneille. Haluttiin siis käytännön esimerkkejä, joita voitaisiin korjata pienellä budjetilla.

### 5.1 Tietoturvakartoituksen huomioita

Auditoinnissa huomattiin muutama vakava poikkeama. Pk-yritys ei ollut selvillä omasta tietoturvantasostaan, koska heillä ei ollut selvää tietoturvapolitiikkaa, eikä riskinhallinnan menettelyn prosesseja ollut laitettu kirjalliseen muotoon. Yleiset toimintaohjeet ja yhteiset käytännöt puuttuivat. Myös henkilöstölle yleiset käytännöt olivat epäselviä.

Kyseisessä pk-yrityksessä, jonne tietoturvakartoitus toteutettiin, oltiin varauduttu fyysisiin riskeihin jo nykyisessä tilanteessa. Varkauksiin on varauduttu varashä-

lyttimien avulla. Merkittäviä varkauksia ei yrityksen toiminnan aikana ole sattunut, mutta niihin on kuitenkin hyvä varautua myös jatkossa. Myös yrityksen sijainnin puolesta teollisuusalueella on otollisella ajatellen ryöstöä tai muita fyysisiä uhkia.

Yritys toimii teollisuusalueella, joka on viikonloppuisin ja yöaikaan vailla vakituista asutusta. Myös rekka ja pakettiautoliikenne on niin vilkasta, että ryöstöä tai varkautta ei helposti tunnisteta jakeluautoista ja muista normaaliin toimintaan viittaavista lastaustöistä.

Tulipaloja ei yrityksen toiminnan aikana ole myöskään sattunut. Näihin oli kuitenkin varauduttu paloturvallisuuslain mukaisella suoja- ja sammutuskalustoilla. Sähkölaitteiden sammutusteoriasta ei kuitenkaan ollut tietoa ja varsinainen pelastussuunnitelma vielä puuttui. Tähän on tulossa kuitenkin korjaus laatujärjestelmän käyttöönoton myötä, joten pelastussuunnitelmaa ei tarvinnut käsitellä tarkemmin, vaan se luvattiin hoitaa kuntoon erillisen konsultin avulla.

Vesivahinkoja tai sähkökatkoksia ei ollut yrityksen tietoturvaa ajatellen huomioitu. Kuitenkin tietokoneet oli sijoitettu automaattisesti siten, etteivät ne ole vesiputkien läheisyydessä. Sähkökatkoksiin puolestaan varauduttiin muista syistä tehtävän varmuuskopioinnin kautta.

Yrityksen tiloissa siivous on ulkoistettu siivousyritykselle. Palveluun ei kuitenkaan kuulu tietokoneiden erillinen puhdistus. Tämä tulisikin jatkossa toteuttaa henkilökunnan puitteissa. Tavoitteena olisi, että jokainen koneen haltija puhdistaisi oman tietokoneensa kerran puolessa vuodessa ja siirtäisi koneen lattialta työpöydälle.

Käytännössä tietoturva ei ollut hallinnassa ja tiettyjä rutiineja ei ollut selitetty tietokoneen käyttäjille. Myös henkilöstölle oli epäselvää erilaisten paperien säilyttäminen ja tietoturvariskit.

Paperijäte heitettiin kaikki suoraan paperinkeräykseen, jossa se oli altis varkauksille ja väärinkäytölle. Myös muu vieraan yrityksen ylijäämä ja jätetavara heitet-

tiin esimerkiksi suoraan karkeajätteeseen. Osa tuotteista ja osista saattaa kuitenkin olla salaisia ja ne on suojattava kilpailijoilta.

Tunnistekortit puuttuivat osalta työmiehiä ja ovet olivat auki, vaikka lukossa pitoa edellytettiin. Myös uuden työntekijän oli vaikea saada heti käytännöistä tietoa. Tietoturvasta ja turvallisuudesta vastaavaa henkilöä ei oltu nimetty. Yksi riski oli myös sosiaalinen media, jossa oli kuvia asiakasyrityksen työmaasta.

### 5.2 Korjaavat toimenpide-ehdotukset tietoturvakartoituksen pohjalta

Tietoturvatason ylläpitoon ja vaatimuksiin sekä tietoturvan yleiseen tasoon vaikuttaa yleisesti hyvin paljon nimetty vastuuhenkilö. Ehdotin, että yritykselle nimetään turvallisuusvastaava, joka huolehtii tietoturvasta ja muusta yleisestä turvallisuudesta. Hän voi osallistua myös koulutuksiin ja olla yhteyshenkilö AEO-turvallisuuden jatkokehityksessä.

Fyysiseen turvallisuuteen pitäisi kiinnittää huomiota. Kriittisiä ovat ainakin varkaudet, murrot ja esimerkiksi kriittiset roskat tai ”salaiset” jätetavarat. Kävimme turvallisuutta läpi turvallisuusfirman kanssa koskien hälyttimiä, turvalaitteita ja yrityksen pihaa. Tällä hetkellä yrityksen yleistä turvallisuutta hoidetaan ulkopuolisen vartiointiliikkeen toimesta. Vartijat käyvät yöllä paikan päällä kierroksella, alueelle on asennettu nauhoittava kameravalvonta ja rakennukset on suojattu murtohälyttimillä.

Sovittiin, että laatujärjestelmän kehityksen yhteydessä tehdään turvallisuusohjeet perehdyttämiskansioihin ja kirjallisiksi ohjeiksi. Niihin tulee turvallisuusmallit, mm. tekemäni tietoturvaohje, teoriaa poimittuna lopputyöstäni ja käytännön vinkkejä miten yrityksessä halutaan tietoturvaa hoitaa.

Sovimme, että paperit ja muu kriittinen jäte hoidetaan yhdessä jäteyhtiön kanssa. Yhtiöltä tuodaan vartioitu ja lukittu jäteastia, johon kaikki kriittinen paperijäte jatkossa laitetaan ja yhtiö huolehtii, että jätteet tuhotaan asianmukaisesti. Suuremmista hävitettävistä laitteista ja muusta riskitavarasta sovitaan sitten tapauskohtaisesti.

Fyysinen turvallisuus hoidetaan pitämällä ovet lukossa ja erottelemalla konttori-henkilöiden ja verstas henkilöiden työpisteet. Verstashenkilöt eivät saa mennä atk-tiloihin ja vastaavasti toisinpäin. Tietoturvaohjeet tulostetaan työpisteillä ja varmuuden vuoksi myös verstaan puolelle ilmoitustaululle. Sovittiin myös, että jatkossa tehdään säännöt sosiaalisen median käytölle, ettei esimerkiksi asiakkaan työmaista tai muusta jaeta niissä kuvia tai tietoa edes vahingossa.

Käytännön atk-koulutus ja ohjeistus jäi nimetylle turvallisuusvastaavalle, joka pitää ulkopuolisen it-yrityksen kanssa tietoturva- ja it-asiat kunnossa. Sovittiin, että ulkopuolinen it-yritys käy tarkastamassa toimitilojen kunnon ja ohjelmistot kolmen kuukauden välein. Erilliset turvallisuusauditoinnit ja muu määritellään tarkemmin laatujärjestelmän laadinnan yhteydessä.

Paloturvallisuus, vesivahingot ym. koskien it-laitteita ja verkkoja sovittiin selvitettäviksi paloviranomaisten kanssa seuraavassa palotarkastuksessa ja ulkopuolisen ylläpitoa tekevän it-yrityksen kanssa pikku hiljaa kuntoon.

# 6 JOHTOPÄÄTÖKSET

Tietoturvan merkitys pk-yrityksessä oli ennen selvitykseni toteuttamista jäänyt lähes kokonaan huomioimatta. Merkittävän asiakasyrityksen hakema AEO–sertifikaatti edellyttää koko alihankintaketjun tietoturvatason selvittämistä ja siksi pk-yritykselle toteutettiin heidän toimestaan tietoturva-auditointi. Yleinen turvallisuus ja tietoturva on myös varmasti kilpailuetu vaatimusten kasvaessa markkinoilla.

Asiakasauditoinnin kautta pk-yrityksessä havahduttiin tietoturvan huonoon tasoon ja sitä haluttiin kehittää. Selvittäessäni yrityksen tietoturvaa koin haastavaksi AEO-sertifikaatin asettamien vaatimusten täyttämisen. AEO-sertifikaatista ei löytynyt paljoa täsmällistä tietoa ja yleisellä tasolla tietoturvasta oli vaikea löytää tietoa, joka vastaisi suoraan pk-yrityksen tarpeisiin. AEO-auditoinnissa riskit ja uhkakuvat oli tuotu esiin hyvin seikkaperäisesti ja niistä saatiin täsmällistä tietoa vain alkuauditoinnin virheraportin muodossa. Tämän takia osa vaatimuksista jäi vielä avoimeksi ja odottamaan lopullisen auditoinnin tuomia tuloksia. Uusi auditointi on tulossa vuoden 2013 aikana.

Vasta tehtyäni yritykselle sisäisen tietoturvakartoituksen ja selvittämällä tietoturvan vaatimukset koko ongelman laajuus ymmärrettiin, ettei pelkkä viruksen torjunta työasemassa riitä, vaan hyvä tietoturvan taso vaatii muutoksia jokapäiväisessä työskentelyssä. Tämän takia laadittiin selkeät tietoturvaohjeet työpisteisiin. Tärkeäksi koettiin myös työntekijöiden mukaan ottaminen ja jatkuva informointi, että saatiin yhdessä toimimisen henkeä mukaan. Turvallisuus kuitenkin koskee koko työpaikkaa.

Selvityksen jälkeen yrityksen atk-laitteistoon tehtiin muutoksia. Kaikki työasemat uusittiin ja aloitettiin puhtaalta pöydältä. Varmuuskopiot ovat tuplavarmistettuna eri verkkolevyillä ja varmuuskopio lähtee myös verkkoa pitkin päivittäin ulkopuoliseen konesaliin. Tietoverkkoa nopeutettiin huomattavasti vaihtamalla adsl-liittymä kuituliittymään. Virustorjuntaohjelmistot uusittiin ja uusi palomuuri ostettiin erillisenä palveluna. Myös tilasuojaus parani, koska ulko-ovet ovat lukittuina ja atk-huoneen ovet pysyvät kiinni aina, kun siellä ei ole henkilökuntaa.

Tärkeäksi työni teki tietoturvatason selvittäminen, koska se oli ehto yritysten välisen yhteistyön jatkumiselle. Lisäksi selkeät toimintaohjeet selkeyttivät ja yhdistivät yrityksen sisäistä toimintaa. Tavoitteena oli luoda vähän paremmat ja helpommin hallittavat toimintatavat, joissa on valmiiksi huomioitu tietoturva.

Mielestäni yrityksen tietoturvan taso nousi selvityksen tekemisen jälkeen ja sitä kehitetään varmasti vielä lisää asiakasyrityksen seuraavan auditoinnin pohjalta. Lähtökohdat ovat kuitenkin paremmat, koska yleiset tietoturvavaatimukset alkavat olla selvillä.

Loppuvaiheessa myös selvisi, että yritys lähti valmistelemaan laatujärjestelmän luontia ja käyttöönottoa. Dokumentoimani asiat ovat varmasti apuna sen laadinnassa ja koko selvitystyöni materiaali on laatujärjestelmän laatimisen tukena.

# LÄHTEET

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki. Edita Publishing Oy.

Matti Laakso.2013.Tietojesi turvaksi. Ohjelmistoturvallisuus. Viitattu 4.5.2013

Paavilainen, J. 1998. Tietoturva. Espoo. Suomen Atk- kustannus Oy.

Tietoturvakartoitus-kysymyslista. Yrityksen tietoturvaopas. Viitattu 25.3.2013 http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvakartoitus_kysymyslista.pdf

Tullihallitus 13.3.2013. AEO- valtuutettu talouden toimija. Viitattu 15.4.2013. http://www.tulli.fi/fi/yrityksille/asiakkaana_tullissa/AEO/

Liite 1. Tietoturvaohje

## 1. Oman verkon suojaaminen

Varmista että asennat aina käyttöjärjestelmän ja ohjelmistojen päivitykset. Tallenna aina keskeneräiset tiedot ja sulje turhat ohjelmat päivittäessä. Käytä aina valmiiksi asennettua ja suojautua etäyhteyttä. Älä koskaan yhdistä omaa laitettasi tai tallennusmediaasi yrityksen verkkoon. Älä lataa tai asenna ohjelmistoja, joita et täysin tunne. Käytä Internetiä vastuullisesti ja harkiten.

---

## 2. Salasanan luonti ja käyttäminen

Pidä kaikki salasanat vain omassa tiedossasi. Älä koskaan kirjoita niitä paperille. Älä käytä työasemassa tai ohjelmissa automaattista salasanan tallennusta,

Käytettävien salasanojen vaatimukset:

Vähintään kahdeksan merkkiä pitkä.

Ei saa sisältää käyttäjätunnusta, oikeaa nimeäsi tai yrityksesi nimeä.

Sen pitää aina poiketa huomattavasti vanhasta salasanastasi

Se sisältää kaikkia seuraavien ryhmien merkkejä:

isot ja/tai pienet kirjaimet

numerot

symbolit (!,@,#,$,% jne.).

---

## 3. Jaetut tiedostot ja yhteisesti käytetyt asemat

Sisäverkossamme on annettu valmiit oikeudet käyttäjille verkkokansioihin. Löydät nimelläsi palvelimelta ”oman kansiosi” tähän vain sinulla on pääsy. Älä koskaan jaa mitään omia tiedostojasi

tai kansioita muille. Yhteisesti käytettävät tiedostot löytyvät ”Yhteiset” kansiosta. Käytä tätä yhteisten tiedostojen jakamiseen.

---

## 4. Työasemasi tietosuoja

Jos poistut työpöytäsi äärestä hetkeksi, varmista, että tietokoneesi on lukittu.

**Tietokoneen lukitseminen:**

Paina näppäimistön näppäimiä CTRL+ALT+DEL samanaikaisesti.

Valitse **Lukitse tämä tietokone** (**Lukitse tietokone**).

Kun haluat poistaa tietokoneen lukituksen, paina CTRL+ALT+DEL-näppäinyhdistelmää ja anna salasanasi.

Kun poistut työpisteesi huoneesta muista aina myös lukita ovi, ettei kukaan pääse työasemasi luo. Älä koskaan jätä mitään tärkeitä papereita työpöydällesi. Laita ne aina lukittuun laatikkoon.

---

## 5. Sähköposti

Jos sähköpostiviesti vaikuttaa epäilyttävältä, epäilykseen on todennäköisesti aihetta. Älä avaa tällaista viestiä, vaan lähetä se edelleen järjestelmänvalvojalle tutkittavaksi. Selvät roskapostit voit ”merkitä roskapostiksi.” Huomaa kuitenkin, että joku saapuva tärkeä viesti on voinut mennä automaattisesti roskapostikansioon.

Jos lähetät luottamuksellista tai liiketoiminnan kannalta arkakaluontoista tietoa muista käyttää salausta.

Älä käytä työsähköpostiasi henkilökohtaisten asioiden hoitamiseen. Äläkä koskaan jaa turhaan verkossa sähköpostiosoitettasi, se saattaa joutua roskapostilistalle.

Lähde: **10 tapaa työskennellä tuvallisemmin. Microsoft yrityksille verkkosivut. 2011.Viitattu 26.3.2013. http://www.microsoft.com/business/fi-fi/Content/Sivut/**

Liite 2. **Tietoturvakartoitus kysymyslista**

# “Tietoturvakartoitus-kysymyslista

1. Mikä on yritykselle arvokasta tietoa?
2. Mikä on yritykselle elintärkeän arvokasta tietoa?
3. Kuinka tietoja valvotaan?
4. Mitä tietoa tarvitaan päivittäin?
5. Mitä tietoa tarvitaan kuukausittain tai harvemmin?
6. Onko yritykselle tehty tietoturvan riskianalyysi?
7. Jos yrityksen tietokone varastetaan, voiko joku hyödyntää siinä olevaa tietoa?
8. Jos tapahtuu sähkönjakeluhäiriö, voivatko päivän aikana luodut tiedostot hävitä?
9. Jos kiinteistössä syttyy tulipalo, voivatko tiedot tuhoutua ja liiketoiminta pysähtyä?
10. Jos tietokone ei tunnista käyttäjää, voiko konetta käyttää petokselliseen toimintaan?
11. Onko etätyön tietoturvasta huolehdittu?
12. Jos työntekijä kertoo junassa tutulleen tuotekehityksen tuloksista, voiko tieto olla merkittävä takana istuvalle kilpailijalle?
13. Jos yrityksessä työskentelevä ulkopuolinen työntekijä kuljettaa tietoa ulkopuolelle, voivatko tiedot joutua niitä hyödyntäville tahoille?
14. Jos työntekijä irtisanotaan, voiko hän tuhota tärkeitä tietoja tai viedä ne eteenpäin ja hyötyä niistä?
15. Onko turvallisuuden kehittämistarpeet tunnistettu?
16. Onko turvallisuuden kehittämistarpeet kirjattu kehittämissuunnitelmaksi?
17. Onko yrityksellänne selkeä johdon hyväksymä tietoturvapolitiikka?

18. Onko kehittämiskustannukset arvioitu?
19. Onko päätetty miltä osin toiminta vakuutetaan?
20. Onko henkilökunta perehdytetty yrityksen tietoturvan käytäntöihin?
21. Onko tietoturvavastuut määritelty?
22. Onko tehtävät vastuutettu?
23. Miten huolehditaan tärkeiden tehtävien varahenkilöjärjestelyistä?
24. Saako jokainen työntekijä käyttöoikeudet vain niihin tietoihin, joita työtehtävä edellyttää?
25. Miten toimitaan, jos epäillään väärinkäytöksiä?
26. Kuinka usein varmistetaan palautusten,varmenteiden ja varajärjestelmien toimivuus?
27. Missä tilanteissa käytetään sähköpostiviestien salakirjoitusmenetelmiä?
28. Säilytetäänkö turvakopiot eri kiinteistössä?
29. Mikä on yrityksenne tietoturvan tilanne tänään?

## Pohdintakysymyksiä henkilötietojen käsittelyyn liittyen

30. Käsitteleekö yritys henkilötietoja?
31. Käsitteleekö se niitä itsenäisenä rekisterinpitäjänä vai toimeksiannosta toisen lukuun?
32. Onko henkilötietojen käsittelyn tarkoitus ja siihen liittyvät prosessit suunniteltu henkilötietolain(523/1999) 6 §:n edellyttämällä tavalla?
33. Onko henkilötietojen suojaamisesta huolehdittu kaikissa niiden käsittelyvaiheissa (sekä sähköisen että manuaalisen aineiston osalta)?
34. Onko työntekijät perehdytetty henkilötietojen käsittelyyn ja siihen liittyviin vastuisiin (mm. salassapito- ja vaitiolovelvollisuuteen)? ”

(http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/pdf/Tietoturvakartoitus_kysymyslista.pdf)